STATUS OF CLAIMS

Claim 1 is pending.

Claim 1 stands rejected.

New Claims 33-43 have been added herein without prejudice.

REMARKS

New Claims

Applicant has added new dependent Claims 33-43, without prejudice, herein. These new claims correspond to previously pending claims 2-12, respectively, which were cancelled without prejudice to simplify the issues for the prior appeal. Accordingly, no new matter has been added.

35 U.S.C. 102(e) Rejection

Claim 1 stands rejected under 35 U.S.C. 102(b) as being anticipated by Feinberg (United States Patent No. 6,065,046). This rejection is traversed, as the cited art of record fails to disclose or suggest each of the features and limitations recited in the present claim.

Claim 1 recites, "[a] method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network." An exemplary block-diagram illustrating such a process is shown in Fig. 3 of the subject application.

The claimed method comprises "extracting a data value from one of said message data blocks." This is explained in the subject application, with reference to

Fig. 3, and the accompanying text, which recites that "the transmitting party extracts a known number of bits from a known position within a message data block at step 410". *Specification, page 7, lines 9-11.* By way of further, non-limiting explanation, this step is also discussed on page 6, in lines 3-7 of the subject application, which discloses that the last data byte of a message data block may be extracted.

The claimed method further comprises, "selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value." This is explained in the subject application, again with reference to Fig. 3, by the accompanying text which teaches that encryption codes are selected at steps 465, 455, 445, 435 based upon comparing the extracted data to some predetermined criteria. *See, Specification, page 7, line 19 – page 8, line 16 ("[a]t block 415 a determination is made whether the value of the extracted data is less than four. If the determination is in the positive, then one of the encryption keys is selected, at block 465 ...").*

Finally, the claimed method comprises "encrypting a subsequent one of said message data blocks using said selected encryption key". This is explained in the subject application, again with reference to Fig. 3, by the accompanying text, wherein "a transmitting party transmits an encrypted message block ... using an encryption key represented as E(x). ... In [the] illustrative embodiment of the invention encryption key E(x) is determined from the data content of a previous message block". *Specification, page 5, lines 14-17.*

In order to anticipate Claim 1, Feinberg must disclose each of the above-identified limitations, including the limitation that <u>a subsequent message data block is</u>

encrypted using an encryption key selected on the basis of the content of a previous message block.

In contradistinction to the claimed invention, Feinberg merely teaches deciphering an encryption packet dependently upon a key identified in the encryption packet header thereof.

More particularly, the Office action relies upon: (1) that portion of Feinberg extending from line 58 in column 11 through line 13 of column 12; and (2) that portion of Feinberg extending between lines 50-59 of column 12, as teaching the recited process of Claim 1. *See, 1/13/2006 Office action, par. 4.* However, a detailed reading of these passages reveals they merely discloses that code modules and data files may be transmitted to a server in an encrypted form by being placed within a "data area" of an encrypted packet. *See, col. 11, lines 58-62.* Further, when an encrypted packet is received by the server, a key that is "identified by header information in the encryption packet" is selected for deciphering. *See, col. 11, line 62- col. 12, line 2.* Thus, the first relied upon portion of Feinberg merely teaches that some value may be identified within a packet header, and used to select a deciphering key for that packet. *See, e.g., col. 12, lines 10-13 ("The header of an encryption packet contains an indication of which plug-in encryption code module must be used for decryption purposes.").* In other words, this passage simply teaches a value may be identified to select a deciphering key, as opposed to an encryption key as is recited by Claim 1.

Further, lines 50-59 of column 12 of Feinberg merely teach that encryption/decryption unit 60 Feinberg "inserts" data requests and information transfer packets into the data portions of encryption packets. Thus, this second relied upon portion of Feinberg likewise fails to teach extracting a data value to select an encryption key.

In view of the foregoing, it is clear that Feinberg fails to teach: (1) extracting a data value from one of said message data blocks; (2) selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and, (3) encrypting a subsequent one of said message data blocks using said selected encryption key – as are recited by Claim 1. Furthermore, Feinberg instead teaches selecting an encryption key identified in received header information, and deciphering the encryption packets. In other words, Feinberg does not teach encrypting a subsequent message block using a key selected dependently upon data extracted from a previous message block.

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1.

For purposes of completeness, Applicant submits Feinberg similarly fails to teach or suggest all of the limitations of dependent Claims 33-43. For example, Feinberg fails to further teach extracting, selecting and encrypting steps are iteratively repeated for each of the message blocks, as is recited by Claim 33. Claims 34-43 are likewise patentable for at least the reasons associated with independent Claim 1. Allowance of these claims is respectfully requested.

Conclusion

Applicant believes he has addressed all outstanding grounds raised in the present Office action, and respectfully submits the present case is in condition for allowance, early notification of which is earnestly solicited.

Should there be any questions or outstanding matters, the Examiner is cordially invited and requested to contact Applicant's undersigned attorney at his number listed below.

Respectfully submitted,

Dated: April 11, 2006

Edward J. Howard
Registration No. 42,670

Plevy, Howard & Darcy, P.C.
PO Box 226
Fort Washington, PA 19034
Tel: (215) 542-5824
Fax: (215) 542-5825